Quantum Key Distribution Services

recent developments and state-of-the-art

7th ETSI Security Workshop, 18-19 Jan 2012

Thomas Länger | AIT | Safety & Security | Quantum Technologies

v9a

Outline of the Talk

Part 1 – QKD basics / recent developments

- Status of ETSI ISG-QKD
- QKD as cryptographic primitive / Security properties of QKD
- Improvement of systems and components

Part 2 – Status of standardization group ISG-QKD

- Security certification framework
  - Security analysis and certification of QKD systems
  - Practical security certification scheme for QKD systems
- Reference model for business application
  - Motivations for using QKD, customers of QKD
  - Services employing QKD

ISG-QKD members
from 11 (10/2008) to 21 (12/2011)

- Research centres
  - Austrian Institute of Technology (AIT)
  - Institut Telecom (FR)
  - Istituto Nazionale di Ricerca Metrologica (INRIM) (IT)
  - Mimos BERHAD (MY)
  - National Institute of Information and Communications Technology (NICT) (JP)
  - Physikalisch-Technische Bundesanstalt (DE) --- NEW!
  - Tubitak Uekae (TR)
- Universities
  - Universidad Politecnica de Madrid (ES)
  - Quantum Works (CD)
- Large Enterprises
  - Qinetiq PLC (UK)
  - Hewlett-Packard, Centre de Compétences France (FR)
  - Thales (FR)
  - Toshiba Research Europe (UK)
  - Mitsubishi Electric RCE (JP)
  - NTT Corporation (JP)
  - Telcordia Technologies, Inc. (US)
- Carriers
  - Swisscom SA
  - Telefonica S.A. (ES)
  - SK Telecom (South Korea) --- NEW!
- SMEs
  - id Quantique SA (CH)
  - Arche Finanz GmbH (DE)

AUSTRIAN INSTITUTE OF TECHNOLOGY

Status of standardization group ISG-QKD

- Operative for three years now; 11 meetings; five standards published
- Focus now on practical security certification and on qualification and measurement of components (as basis for security proofs/security certification)
- New ISG members from metrology domain (NPL (GB), PTB (D), INRIM(I))
- New EMRP (European Metrology Research Program) project

  MIQC "Metrology for Industrial Quantum Communication Technologies"
- They work on basis of ETSI GS 003 "Components and Internal Interfaces" and will improve it (dedicated work package) -> important for security certification!

- Funding standardization work through external projects...

  ...**is that the way to "run" an ISG for a still research centered topic.......?**

A look at QKD as cryptographic primitives

cryptographic primitives are low level building blocks for implementing cryptographic services:

- encryption (confidentiality)
- authentication (integrity, proof of origin)
- **key distribution → Quantum Key Distribution QKD**
- digital signature scheme (proof of origin, integrity, non repudiation)
- + other primitives for commitment schemes, oblivious transfer...

For each primitive exist different “flavours” with different security levels

Security "levels" of cryptographic primitives

- **Computational security** (key distribution): there is a lower bound on the number of operations necessary to break the key distribution primitive. Achieving the bound is beyond current technology (Example: DH...)

- **Information theoretical security (ε–ITS)** (key distribution): the amount of information on the key is (for non legitimate parties) upper bounded by a constant $\varepsilon > 0$ during key distribution. ε can be made arbitrarily small (ε possibly 2^{-100})

- **Perfect security** (encryption primitive): probability to get ciphertext *C* is exactly the same for all possible plaintext messages M_i, that is C gives exactly zero information about the plaintext (even with unlimited computing power)

$$\text{plaintext} \xrightarrow[\text{cipher and key}]{\text{encrypt with}} \begin{array}{c}\text{ciphertext}\\ \text{or cryptogram}\end{array} \xrightarrow[\text{cipher and key}]{\text{decrypt with}} \text{plaintext}$$

Quantum Key Distribution is ITS

- QKD is an “almost ideal realization” of an ε-ITS key distribution primitive
  - the system generates key between two distant locations connected by a classical and quantum communication channel
  - no information available to the eavesdropper except for a leakage bounded by ε_1
  - key correctness: the probability that the key between the two parties is not identical is limited by ε_2
  - system robustness: the probability that the system fails to generate key in the absence of an eavesdropper is limited by ε_3 (this probability needs not be very low)
  - the total security parameter of the system is $\varepsilon = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$. The system (the model QKD protocol) can be combined with other ε-ITS-secure protocols to yield ε-ITS-secure higher order applications

Specific security properties of (ITS) QKD systems

- Not only gradually “higher” security - Fundamentally different kind of security
- No speedup in computer technology (quantum computer)
  will put QKD out of business
- QKD has “forward security” – a securely established key will by no means be compromised in the future

- Yes, implementations of QKD have side channels (quantum hacking)
  (like any other security ICT system implementation)
- QKD even has additional side channels related to its optical subsystem
- Side channels can be controlled.

- It may occur that QKD systems (specific implementations) be compromised.
- But QKD by itself, as method, will not be compromised

Improvement of systems and components

- Detectors: performance improvement 100-1000 times between 2008 and 2010 (new self differencing circuit allows clock rates > 1GHz with InGaAs APD)

- Post Processing: performance improvement 10-100 times through application of LDPC error correction (instead of cascade)

- Miniaturization (integrated optics)

- WDM integration (multiple quantum channels in different colours on one fibre) (reconfigurable network, addressing...)

ISG-QKD has two main goals

Goal #1: Enable dependable practical application of QKD as part of security solutions by developing standards:

- for the qualification of QKD system components
- for the security certification of entire QKD systems

  (as well as standards for interfaces, system management)

Goal #2: foster market creation by developing reference model for business application:

- Develop use cases for QKD application and showcasing its added value for security system

ISG-QKD Goal #1: Development of security certification scheme for QKD

- Proposal of new scheme for practical security certification is currently being developed in the ETSI ISG-QKD (QKD#11 Nov 30 – Dec 2, 2011)
- An evolutionary practical approach is carried out on the basis of a single system type/implementation that is well understood
- In order to better understand the process, initial results shall be produced
- Attempt to modify / rewrite GS QKD 005 „QKD; Security Proofs“ so that these issues are covered sufficiently

- Additional work is carried out for the qualification of QKD components

ISG-QKD Goal#1: Development of security certification scheme for QKD (continued)

- Use existing security proof for the corresponding idealized system
- Summarize all relevant components for this system and analyze the possible imperfections (in model form?)
- Subsequently try to extend the idealized model to cover these imperfections or /and (for large deviations)
- Make reasonable conjectures and introduce countermeasures based on existing results and attacks
- On this basis try to formulate a detailed generic catalogue for security standardization
- Translate assumptions, conjectures, missing proofs to limitations on the eavesdropper; the security specification then will be:
  - ε-ITS secure with a set of defined assumptions, conjectures, etc. OR
  - secure against eavesdropper of well defined power

ISG-QKD Goal #2: Development of reference model for business application

- Analyze motivations for using QKD
- Find customers of QKD
- Present several services employing QKD
  - fiber based
  - free space (satellite) based
- Analyze drivers and inhibitors of QKD development

Motivations for using QKD

- Requirement of long term confidentiality (forward security)
  - Government, defence
  - Medical data, health data, genetic codes
  - Personal data (private data)
- Highest security requirements
  - Critical information - when a break leads to unrecoverable disaster
- Additional Motivations
  - Efficient solution for highest security standards
  - Competitive and reputation advantage (confidence)
  - Alternative solution for demanding users
  - Being in regulatory conformity

Customers of QKD I

- There are different groups of customers
- Not precisely/unambiguously defined who the customers are
- Multiple “stages” of customers/users

- **1. Owners (**of systems and communication infrastructures)
  - Governments
  - Military agencies
  - Critical Infrastructures
  - Financial entities
  - Businesses (e.g. Airports)

Customers of QKD II

- **<u>2. End users</u>** who buy a service from a **<u>service provider</u>**
  - Enterprises (large, medium, small)
  - Private individuals
  - Possibly also entities from the Owners group…
- **<u>3. The “community”, unions of member states, governments</u>**
  - Ultimate future goal: to have reliable, resilient information infrastructures serving the Information Society. A “New Internet” needs:
    - Suitable protocols for current and future use (by overlay networks)
    - Wider address space
    - Energy saving implementation
    - Integrated security features
  - Put QKD in a backbone; make it a standard for the backbone (QKD has e.g. a slot in Japanese “new-generation-networks” initiative)

QKD based services

- We focus here on the 2nd group:
  <u>nd users</u> who buy a service from a **<u>service provider</u>** (telecom perspective)

- Two “principal” types of services

  - Type 1: “Plain secret key distribution” …to be used in any type of security application

  - Type 2: Integration with “classical” communication channel, in order to secure payload transmissions with the generated quantum keys

    - here: elaborate on principal resource – quantum channel
    - compatibility with typical fiber lengths in metro networks

Examples of QKD based services (non exhaustive)

- Lease a secure communication line (Type 2)

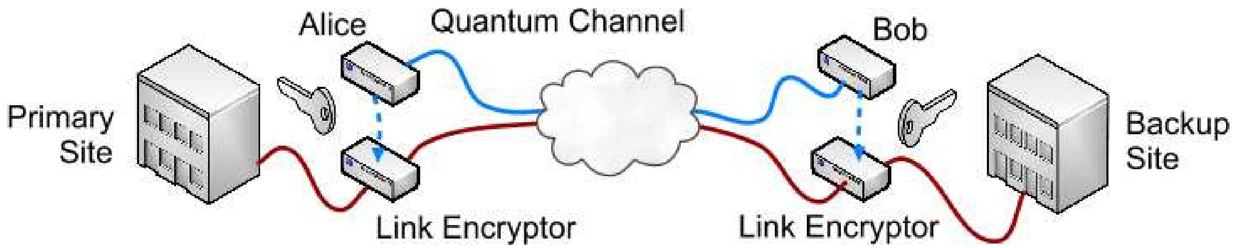
  - Use Case 1: Offsite backup / business continuity
  - Use Case 2: Highly secure government communicaton network
  - Use Case 3: High security access network

- Buy secret keys (Type 1)

  - Use Case 4: Continental scale secret key delivery (satellite QKD)
  - Use Case 5: World-wide secret key delivery (satellite QKD, with trust assumption)

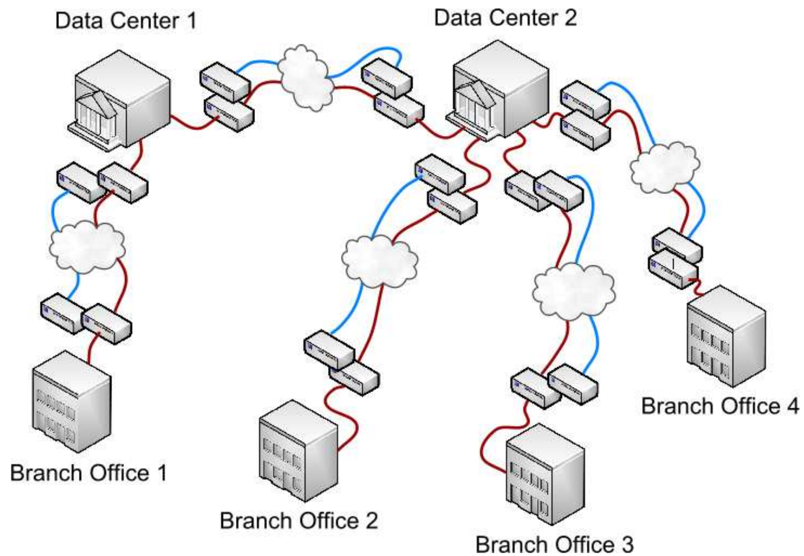
Use Case 1 “Off-site backup / business continuity”

- protection of backup or database replication
- encrypted tunnel between two data centers
- customer leases/buys QKD equipment, leases quantum channel
- compatible with distances required through regulation
- is already implemented (Geneva-Lausanne)
- advantages…..



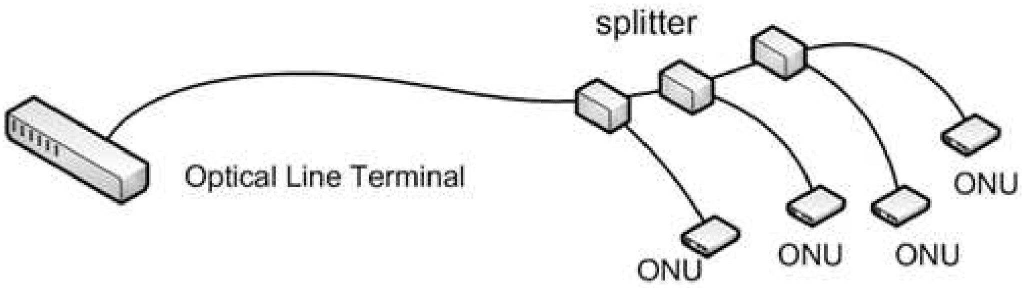
Use Case 2 “Highly secure government communication network”

- interconnect government sites in metropolitan area
- government leases secure tunnel from „federal data processing center“
- different grades of security for different applications (according to security requirements)
- has a „classical“ equivalent today



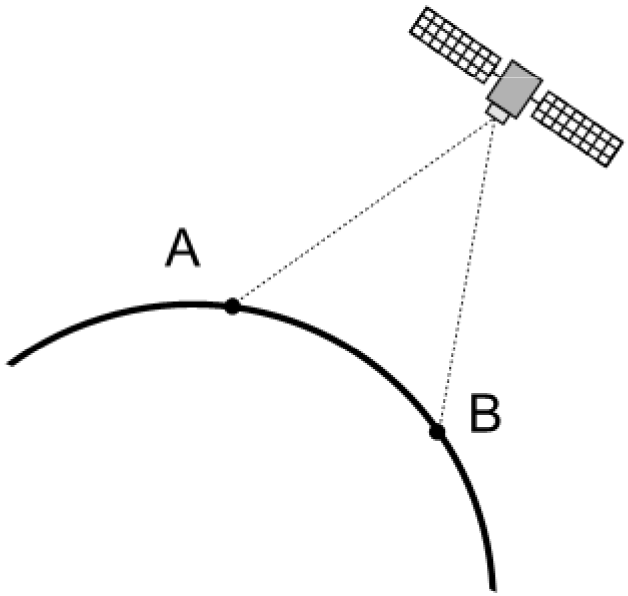
Use Case 3 “High security access network”

- secure an access network (PON), e.g. inside an office building
- PON is also transparent for quantum information
- cryptographically isolate the optical network units of the single end users
- service may be leased from facility provider



Use Case 4 “Continental scale secret key delivery”

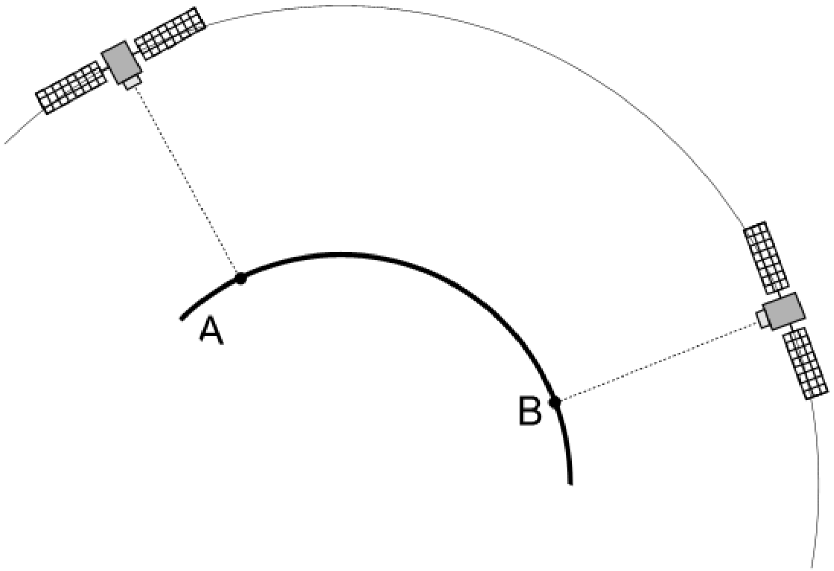
- key distribution on a continental scale to end users
- using entanglement distribution
- from a single satellite
- satellite needs not to be trusted
- post processing carried out on ground
- sites do not have to rely on availability of fibers



Use Case 5 “World-wide secret key delivery”

- world-wide key distribution to end users
- using prepare and measure QKD
- from a moving single satellite
- with sequential access
- satellite needs to be trusted

  (trust assumption)



THOMAS LÄNGER

Safety & Security Department
Quantum Technologies

AIT Austrian Institute of Technology GmbH
Donau-City-Straße 1 | 1220 Vienna | Austria
thomas.laenger@ait.ac.at | http://www.ait.ac.at